DGR:BDM
F.#: 2023V04176

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
– X

UNITED STATES OF AMERICA,

Plaintiff,

-against-

APPROXIMATELY FIVE HUNDRED FORTY-ONE THOUSAND NINE HUNDRED FIFTY-THREE DOLLARS AND ZERO CENTS ($541,953.00) SEIZED FROM JP MORGAN CHASE NA ACCOUNT NUMBER 928805297 HELD IN THE NAME OF JIAWIG TRADE INC, AND ALL PROCEEDS TRACEABLE THERETO.

Defendant in rem.

– X

VERIFIED COMPLAINT
IN REM

Civil Action No. 23-CV-9585

Plaintiff, the United States of America, by its attorney, BREON PEACE, United States Attorney for the Eastern District of New York, alleges upon information and belief as follows:

PRELIMINARY STATEMENT

1. This is a civil action in rem to forfeit and condemn to the use of the United States the above-captioned defendant funds (the "Defendant Funds"), in accordance with: (a) 18 U.S.C. § 981(a)(1)(C), as property constituting or derived from proceeds of a wire fraud scheme, in violation of 18 U.S.C. § 1343; and (b) 18 U.S.C. § 981(a)(1)(A), as property, real or personal, involved in a transaction or attempted transaction in violation of 18 U.S.C. § 1956, or property traceable to such property.

JURISDICTION AND VENUE

2. This Court has jurisdiction over this action pursuant to 28 U.S.C. §§ 1345 and 1355.

3. Venue lies in the Eastern District of New York pursuant to 28 U.S.C. §§ 1355 and 1395, in that acts and omissions giving rise to the forfeiture occurred in Eastern District of New York.

THE DEFENDANT IN REM

4. The Defendant Funds consists of a total of $541,953 seized from JP Morgan Chase NA account number 928805297 held in the name of Jiawig Trade Inc (the "Jiawig Account"), and all proceeds traceable thereto. The Defendant Funds were seized on or about August 1, 2023, pursuant to a warrant issued by United States Magistrate Judge James R. Cho.

STATUTORY BACKGROUND

5. Title 18, United States Code, Section 1343 prohibits any person from devising a scheme or artifice to defraud, and to obtain money or property by means of materially false and fraudulent pretenses, representations, promises, and for purposes of executing such scheme and artifice, to transmit or cause to be transmitted by means of wire communications in interstate and foreign commerce writings, signs, signals, pictures and sounds.

6. Title 18, United States Code, Section 981(a)(1)(C) provides for the forfeiture of any property, real or personal, which constitutes or is derived from proceeds traceable to any offense, or conspiracy to commit such an offense, which constitutes "specified unlawful activity," as defined in Title 18, United States Code, Section 1956(c)(7).

7. Pursuant to Title 18, United States Code, Section 1956(c)(7)(A), which incorporates Title 18, United States Code, Section 1961(1)(B) by reference, the term "specified unlawful activity" includes any criminal offense relating to wire fraud, in violation of Title 18, United States Code, Section 1343.

8. Title 18, United States Code, Sections 1956(a)(1)(B)(i) and 1956(h) prohibit any person knowing that the property involved in a financial transaction represents proceeds of some form of unlawful activity, to conduct or attempt to conduct, a financial transaction which in fact involves the proceeds of specified unlawful activity knowing that the transaction is designed in whole or in part to conceal or disguise, the nature, the location, the source or the ownership or the control of the proceeds of specified unlawful activity, or to conspire to commit such an offense.

9. Title 18, United States Code, Section 981(a)(1)(A) provides for the forfeiture of any property, real or personal, involved in a transaction or attempted transaction in violation of Section 1956, or any property traceable to such property.

10. In any forfeiture action in which the subject property consists of funds deposited into a bank account, the government is not required to identify the particular funds involved in the offense, as any funds found in the same account within one year of the date of the offense are subject to forfeiture pursuant to Title 18, United States Code, Section 984.

CRYPTOCURRENCY BACKGROUND

11. Cryptocurrencies are a type of digital asset that can act as a decentralized, peer-to-peer, network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency or other

cryptocurrencies. Examples of cryptocurrency are Bitcoin, Ether, and Tether. Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud-based servers. Although not usually stored in any physical form, public and private keys (described below) used to transfer cryptocurrency from one person or place to another can be printed or written on a piece of paper. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Generally, cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Most cryptocurrencies have a "blockchain," which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction. Cryptocurrency is not illegal in the United States.

12. Cryptocurrency is stored in a virtual account called a wallet. Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. A public key or address is akin to a bank account number, and a private key is akin to a PIN number or password that allows a user the ability to access and transfer value associated with the public address or key. To conduct transactions on a blockchain, an individual must use the public address (or "public key") and the private address (or "private key"). A public address is represented as a case-sensitive string of letters and numbers, 26 to 36 characters long. Each public address is controlled and/or accessed through the use of a unique corresponding private key—the cryptographic equivalent of a password or PIN— needed to access the address. Only the

holder of an address's private key can authorize any transfers of cryptocurrency from that address to another cryptocurrency address.

Bitcoin

13. Bitcoin ("BTC") is a type of virtual currency, circulated over the Internet. Bitcoin are not issued by any government, bank, or company, but rather are controlled through computer software operating via a decentralized, peer-to-peer network. Bitcoin is just one of many varieties of virtual currency.

14. Bitcoin are sent to and received from Bitcoin "addresses." A Bitcoin address is somewhat analogous to a bank account number and is represented as a case-sensitive string of letters and numbers of a specified length.

15. Each Bitcoin address is controlled through the use of a unique corresponding private key. This key is the equivalent of a password, or PIN, and is necessary to effectuate transfers of the funds associated with a Bitcoin address. Only the holder(s) of the private key can authorize transfers of Bitcoin from that address to other Bitcoin addresses. Users can operate multiple Bitcoin addresses at any given time and may use a unique Bitcoin address for each transaction.

16. There are multiple ways to acquire Bitcoin, but a typical way is through purchases of Bitcoin from a virtual currency exchange. A virtual currency exchange is a business that allows customers to trade virtual currencies for other virtual currencies or other forms of value, such as conventional fiat money (e.g., U.S. dollars, Russian rubles, euros). Exchanges can be brick-and-mortar businesses (exchanging traditional payment methods and virtual currencies) or online businesses (exchanging electronically transferred money and virtual currencies). Virtual currency exchanges doing business in the United States are

regulated under the Bank Secrecy Act and must collect identifying information about their customers and verify their clients' identities.

17. To transfer Bitcoin to a different Bitcoin address, the sender transmits a transaction announcement, which is electronically signed with the sender's private key, across the peer-to-peer Bitcoin network. To complete a transaction, a sender needs only the Bitcoin address of the receiving party and the sender's own private key. This information on its own rarely reflects any identifying information about either the sender or the recipient. As a result, little-to-no personally identifiable information about the sender or recipient is transmitted in a Bitcoin transaction itself. Once the sender's transaction announcement is verified by the network, the transaction is added to the blockchain, a decentralized public ledger that records every Bitcoin transaction. The blockchain logs every Bitcoin address that has ever received Bitcoin and maintains records of every transaction for each Bitcoin address.

18. While a Bitcoin address owner's identity is generally anonymous within the blockchain (unless the owner opts to make information about the owner's Bitcoin address publicly available), investigators can use the blockchain to identify the owner of a particular Bitcoin address. Because the blockchain serves as a searchable public ledger of every Bitcoin transaction, investigators can trace transactions to, among other recipients, Bitcoin exchangers. Because Bitcoin exchangers generally collect identifying information about their customers, as discussed above, subpoenas or other appropriate legal process submitted to exchangers can, in some instances, reveal the true identity of an individual responsible for a Bitcoin transaction.

Ethereum

19. The Ethereum blockchain is a distinct blockchain from Bitcoin with its own native cryptocurrency also called Ethereum, which shares many similarities with Bitcoin.

20. Like Bitcoin, Ethereum is a digital asset or cryptocurrency traded through online exchanges and stored in various cryptocurrency wallets.

21. Both Bitcoin and Ethereum are decentralized and are not issued or regulated by any central banks or other authorities.

22. Both make use of the distributed ledger technology known as blockchain.

23. One of the significant differences between Bitcoin and Ethereum is that the latter comes complete with its own programming language, which runs on blockchain, and which enables developers to build and run decentralized websites and applications on Ethereum.

24. Another difference between Bitcoin and Ethereum is that computer protocols, often referred to as "smart contracts" can be used on the Ethereum blockchain. These "smart contracts" are self-executing lines of code that are used to ensure that a contract between parties executes as expected on agreed upon terms.

Tether

25. Tether ("USDT") was founded in 2014 and is another cryptocurrency like Bitcoin and Ethereum.

26. Like Bitcoin, Tether is a blockchain-based virtual currency that is widely used and circulated over the Internet. However, unlike Bitcoin, Tether is a

"stablecoin" which is a type of cryptocurrency that aims to keep cryptocurrency valuations stable and pegged to a particular asset in the non-digital world, such as the U.S. dollar or gold. Tether is designed to be pegged to the U.S. dollar such that 1 Tether is equal to 1 U.S. dollar. Tether is backed by reserves in fiat currency. Tether and other stablecoins are primarily utilized by cryptocurrency investors who want to avoid the extreme volatility of other cryptocurrencies while keeping value within the cryptocurrency market.

FACTS

27. The USSS has investigated a form of investment fraud, which utilizes fraudulent investment and/or cryptocurrency trading applications (hereinafter "Fraudulent Investment Platforms") designed to convince users that they are popular investment and/or cryptocurrency trading platforms into which their cryptocurrency or fiat currency can be deposited. These Fraudulent Investment Platforms aim to take advantage of the increasing interest individuals have in cryptocurrency, and who are looking to capitalize on the rise of cryptocurrency value as well looking to invest in legitimate cryptocurrency trading platforms, which offer low cost and often yield high returns on cryptocurrency trading. To accomplish this, the Fraudulent Investment Platforms often use web addresses or application software that appear similar to those of actual cryptocurrency exchanges or other investment brokerages to help conceal the true nature of the platforms. Although posing as the legitimate and widely used investment and trading platforms, in reality, the Fraudulent Investment Platforms are controlled by third parties.

28. The purpose of the Fraudulent Investment Platforms is to allow these third parties to facilitate the theft of crypto and fiat assets from victims tricked into sending

funds to the websites or applications. The platforms display false balances and values of cryptocurrency or other earnings, falsely indicating that the cryptocurrency and/or fiat assets are being held for the victim and increasing in value. In reality, the crypto and/or fiat assets transferred by the victim have already been diverted. The Fraudulent Investment Platforms also provide victims with a dedicated "customer service" portal designed to further impersonate a trading company brand, as well as stall, prevent, and further steal funds from victims when they attempt withdraw their funds. For example, the "customer service" portals typically require victims to wait a certain period before withdrawing or require victims to deposit additional funds in order to withdraw their cryptocurrency and/or fiat currency.

29. In April 2023, the USSS uncovered multiple victims within the United States, including within the Eastern District of New York, who have sent money to various Fraudulent Investment Platforms and websites purporting to be legitimate cryptocurrency exchanges and/or investment platforms. In addition to sending funds to invest in cryptocurrency, victims were also convinced to wire fiat currency to various fraudulent companies on the belief that they were investing in gold and/or cryptocurrency.

The Scheme to Defraud The Victim

30. On or about April 20, 2023, an individual residing in Hawaii (hereinafter, the "Victim") filed a report on IC3.gov to report that he was the victim of an investment fraud perpetrated by an unknown individual.

31. Thereafter, on or about June 7, 2023, the Victim was interviewed by law enforcement agents regarding his complaint and reported the following in sum, substance, and in part:

a. On or around January 1, 2023, the Victim received a text from an unknown woman who identified herself as Qiu Jiaxin and claimed to live in Singapore (hereinafter "UF-1"). Soon thereafter, UF-1 requested that they communicate via "Telegram" instead. Victim-2 complied.

b. UF-1 told Victim-2 that she made extreme profits by investing in gold and cryptocurrency. Moreover, UF-1 told Victim-2 that she could help him do the same. On or around January 6, 2023, UF-1 demonstrated how to make money by utilizing foreign currency exchange rates on gold and cryptocurrency using the platform "Sundell-fx.com" (hereinafter, the "Fraudulent Investment Platform"). UF-1 instructed Victim-2 to use that website to download the "FX6" application, which he used to see his purported earnings.

c. On or about April 12, 2023, the Victim attempted to withdraw his earned profits but was denied by purported customer service representatives, stating that Victim-2 needed to pay "5% tax to UK Tax Agency due by May 5 2023" and that he would owe an extra 1% each day he was late.

32. Law enforcement agents analyzed "Sundell-fx.com" (the Fraudulent Investment Platform) and learned that was still active. Furthermore, "sundell-fx.com" (the Fraudulent Investment Platform) has numerous open-source complaints lodged by customers stating that they were scammed by the platform.

33. Agents also queried "Sundell-fx.com" on WHOIS, and a widely used Internet record listing service, and learned that it was registered on December 6, 2022.

34. As a result of this investment fraud scheme, the Victim was defrauded out of a total of approximately $1,525,000.

The Jiawig Account

35. The Jiawig Account, maintained at JP Morgan Chase, is associated with account number 928805297 held in the name of Jiawig Trade Inc.

36. As set forth infra, law enforcement agents have traced the Victim's funds to the Jiawig Account. In addition, as detailed below, the Jiawig Account has been reported to law enforcement as an account used in other fraudulent schemes.

37. The Jiawig Account was opened online on or about February 23, 2023.

38. According to financial records, the sole signatory on the Jiawig Account is MiaoMiao Zhang.

39. From account inception through the date of seizure, there were roughly 53 incoming wire transfers into the Jiawig Account, totaling approximately $3,497,958. These wires were conducted between March and April 2023.

40. From account inception through the date of seizure, there were roughly 25 outgoing ACH payments from the Jiawig Account, totaling approximately $3,419,900.

41. Law enforcement agents analyzed the business entity associated with the Jiawig Account, "Jiawig Trade Inc.," and learned that it purportedly "sells durable goods such as brushes, storage boxes, hair stickers." Jiawig Trade Inc. was registered to "Farscar Cap Ltd" with MiaoMiao Zhang as the filer on January 19, 2023, in Albany, New York. In addition, Jiawig Trade Inc. has a registration address of 90 State Street, Suite 700, Albany, NY.

42. Law enforcement agents queried Jiawig Trade Inc. using open-source tools and determined that it did not maintain a visible online presence or advertising. Further, a search of the registered address revealed that it is listed as a virtual office space where individuals can use that address to receive mail, register companies, and for marketing purposes.

43. Jiawig Trade Inc. has been named in at least five IC3.gov complaints from victims reporting that they sent funds related to socially engineered wire fraud schemes.

44. Law enforcement agents learned that in or around March 2023, an individual reported that they were a victim of fraud after being contacted by a woman who offered to help them make large profits through trading Bitcoin on "coindcs-us.co." At the instruction of the unknown woman, the individual wired $15,000 to the Jiawig Account.

45. Continuing in or around March 2023, another individual reported that there was a preauthorized charge on her PayPal account that required her verification. The individual called the number provided and was told that she needed to wire $40,000 to the Jiawig Account to retrieve her funds. The individual's bank successfully stopped the wire transfer.

46. Law enforcement agents also learned that in or around March 2023, an individual reported that they were convinced by an unknown woman to engage in foreign currency exchange rate trading. After the individual tried to withdraw profits, he was notified that he owed approximately $111,456. Thus, at the scammer's instruction, the individual wired $111,456 to the Jiawig Account.

Tracing of Victim Funds to the Jiawig Account

47. As set forth above, between February 2, 2023, and March 31, 2023, the Victim transferred approximately $1,525,000 from his TD Ameritrade bank account ending in 9441 and his First Hawaiian bank account ending in 2449 to various bank accounts at the direction of UF-1, and the Fraudulent Investment Platform.

48. On or about March 31, 2023, Victim-2 wired $200,000 from his First Hawaiian account ending in 2449 to the JP Morgan Chase account provided by UF-1, which was the Jiawig Account belonging to "Jiawig Trade Inc."

FIRST CLAIM FOR RELIEF

49. Plaintiff repeats the allegations of paragraphs 1 through 48 as if fully set forth herein.

31. The Defendant Funds constitute and/or are derived, at least in part, from proceeds traceable to wire fraud, a violation of 18 U.S.C. § 1343.

32. As such, the Defendant Funds are subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(C).

SECOND CLAIM FOR RELIEF

33. Plaintiff repeats the allegations of paragraphs 1 through 48 as if fully set forth herein.

34. The Defendant Funds represent property involved in a transaction or attempted transaction in violation of 18 U.S.C. § 1956, or property traceable to such property.

35. As such, the Defendant Funds are subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(A).

Dated: Brooklyn, New York
December 29, 2023

BREON PEACE
UNITED STATES ATTORNEY
Attorney for Plaintiff
Eastern District of New York
271 Cadman Plaza East
Brooklyn, New York 11201

By: /s Brian Morris
Brian D. Morris
Drew G. Rolle
Assistant United States Attorneys
(718) 254-7000

VERIFICATION

Dylan Tucker hereby declares as follows:

1. I am a Special Agent with the United States Secret Service.

2. I have read the verified complaint in rem in this action and know the contents thereof.

3. The matters contained in the within verified complaint in rem are true and accurate to the best of my knowledge, information and belief.

4. The source of my information and the grounds for my belief are my personal knowledge, information provided by other law enforcement officers, and the official files and records of the United States Secret Service and other law enforcement agencies.

I declare under penalty of perjury that the foregoing is true, to the best of my knowledge, information, and belief.

Dated: Brooklyn, New York
December 29, 2023

Dylan Tucker

Dylan Tucker
Special Agent
United States Secret Service